VIGI PRENSA: 2015

Seguridad Smartphone

¿Cómo proteger la información del Smartphone?

Un Smartphone cuenta con un sistema operativo que tiene capacidades de computación avanzada convirtiéndose en un completo computador de bolsillo, en esta clasificación encontramos los equipos de Blackberry, la serie Optimus de LG, iPhone, serie Lumia de la marca Nokia, o los Galaxy de Samsung entre otros.

Lo anterior y dadas las capacidades tecnológicas o funciones que han adquirido los dispositivos móviles durante los últimos años resulta claro el interés que estos sean objeto de atención para los ciberdelincuentes, por ello que a continuación se brindan algunas recomendaciones de seguridad para el uso seguro del Smartphone.

1. Contraseñas: Las contraseñas (acceso al equipo, servicios web, redes sociales y otras aplicaciones) deben tener una configuración robusta como principal norma de seguridad en todo sistema informático para evitar que en caso de hurto o extravío, personas inescrupulosas tengan acceso a la información allí almacenada.
2. Correo electrónico y navegación Web: Los teléfonos móviles pueden llegar a ser infectados por malware o virus con el simple hecho de pinchar un link o abrir un correo electrónico extraño, de igual modo el usuario puede ser víctima de fraude o estafa mediante estos dispositivos. Por lo tanto, es recomendable no abrir correos no deseados o descargar archivos sospechosos al celular. Por otra parte en la medida de las posibilidades usar siempre el cifrado SSL (https://) para navegar en Internet.
3. Redes inalámbricas: Se deben mantener apagadas las opciones de Wi-Fi y Bluetooth activándolas solamente cuando se vaya hacer uso de ellas de otro modo si estas mantienen activas (que en muchos casos ocurre por defecto de configuración del teléfono celular) delincuentes informáticos podrían espiar la red descargando la información de los dispositivos que estén conectados.
4. Aplicaciones: Se deben instalar las aplicaciones que sean necesarias y sólo aquellas que gocen de buena reputación o puntaje. Entre más aplicaciones se instalen más vulnerable es un sistema, asimismo hay que tener en cuenta que los delincuentes crean APPS (aplicaciones) maliciosas para infectar los equipos móviles.

VIGI PRENSA: 2015

5. Actualizaciones: Todo sistema informático debe mantenerse actualizado como parte de una mejora constante a las aplicaciones instaladas teniendo en cuenta que cada día se robustecen o reparan defectos y vulnerabilidades de las mismas.
6. Documentación: Como parte de la seguridad de la información se debe leer las políticas, condiciones o términos de uso de las aplicaciones que se instalan en el SMARTPHONE, ya que algunas solicitan permiso para recolectar, usar y vender la información de registro, información de uso o localización geográfica del usuario.
7. Seguridad física SMARTPHONE: Es recomendable en una parte no tan visible del dispositivo móvil por ejemplo en la pila o en la tapa trasera colocar una etiqueta con los datos de contacto del propietario en caso que este sufra pérdida, también de ser posible activar la geolocalización del celular el cual utiliza el GPS instalado en el dispositivo. Por último, hacer una copia de seguridad o back-up de la información para su eventual restauración es otra medida aconsejable.
8. Borrado: La mayoría de usuarios tienen servicio de red en el Smartphone lo cual permite su configuración de tal modo en caso de sufrir pérdida o hurto el propietario puede realizar un borrado remoto de la información personal almacenada en el dispositivo móvil.
9. Eliminación: Antes de reemplazar un teléfono celular debe eliminar de forma segura la información allí contenida mediante los comandos (código o instrucción) que tiene cada modelo de celular para tal fin, que puede ser consultado con el proveedor de servicio o en el manual de instrucciones.
10. Entorno laboral: Antes de conectar el Smartphone a la red del trabajo o específicamente al correo empresarial se debe consultar y solicitar la respectiva autorización al departamento de tecnología para no infringir alguna regulación legal o para que su información personal no se convierta en objeto auditable de la empresa.

Fuente: Centro Cibernético Policial Nacional/Ministerio de Defensa Nacional-MDN.
http://www.ccp.gov.co/ciberseguridad/recomendaciones/seguridad-smartphone